V této práci se zabýváme šifrovacími schématy, která jsou dokazatelně bezpečná i v případě, kdy šifrujeme zprávy, které závisejí na tajném klíči. Taková schémata nazýváme KDM-bezpečná.

Nejprve zavádíme pojem KDM-bezpečnosti obecně a zkoumáme jeho vztah s jinými druhy bezpečnosti, zejména s IND-CPA-bezpečností. Poté popisujeme asymetrické i symetrické šifrovací schéma autorů Applebaum et al. (CRYPTO 2009) a dokazujeme KDM-bezpečnost těchto schémat s ohledem na množinu afinních funkcí.

Klíčovým předpokladem bezpečnosti sestrojených schémat je těžkost problému LWE, respektive jeho speciálního případu LPN. Tyto problémy blíže zkoumáme a rozebíráme jejich varianty. Dále se věnujeme i mřížkám a těžkým problémům na mřížkách, protože se redukují na problém LWE.